# EXHIBIT #1

MEDICAL DEVICE & DRUG MANUFACTURING LITIGATION GROUP
2006 roundtable series

The ILN is an association of 87 high-quality, full-service law firms with over 5,000 lawyers worldwide. The Network provides clients with easily accessible legal services in 62 countries on six continents.

## Contributors

**MR. STEPHEN C. RATHKE**
Lommen Abdo - Minneapolis
Tel: 612.336.9305
Email: steve@lommen.com

**MR. JEFFREY B. SHAPIRO**
Arnstein & Lehr LLP - Miami
Tel: 305.357.2005
Email: jbshapiro@arnstein.com

**MR. JOSEPH S. COHEN**
Beirne Maynard Parsons LLP
Houston
Tel: 713.960.7312
Email: jcohen@bmpllp.com

**MR. NORMAN ZIVIN**
Cooper & Dunham LLP - New York
Tel: 212.278.0400
Email: nzivin@cooperdunham.com

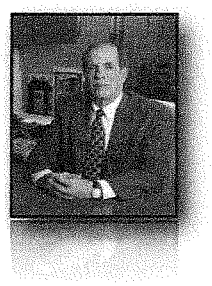
**MR. WILLIAM J. O'NEIL/MATT RECHNER**
McDonald Hopkins Co., LPA
Cleveland
Tel: 216.348.5755
Email: woneill@mcdonaldhopkins.com

**MR. GEOFFREY BRIDGMAN**
Ogden Murphy Wallace - Seattle
Tel: 206.447.7000
Email: gbridgman@omlaw.com

**MR. PAUL GALE**
Stradling Yocca Carlson & Rauth
Newport Beach
Tel: 949.725.4000
Email: pgale@sycr.com

# How to Lose a Lawsuit by Not Keeping Track of Your E-mails and Documents: Spoliation, Electronic Discovery and the Avoidance of Sanctions

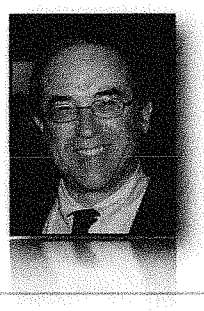
### What is spoliation?



Stephen Rathke: Spoliation is the destruction of evidence. Spoliation may be intentional, negligent or inadvertent. Probably every state has its definitive spoliation case. See, e.g., Federated Mutual Ins. Co. v. Litchfield Precision Components, Inc., 456 N.W.2d 434 (Minn. 1990). Until a few years ago, most spoliation case involved product liability cases and fire scenes. More recently, spoliation issues occur with electronically stored documents.

Joe Cohen: A legal duty to preserve electronic (or any other) evidence must exist before spoliation occurs. Case law varies from jurisdiction to jurisdiction. In general, a duty exists to preserve evidence when litigation is imminent, anticipated, filed, pending, or is reasonably foreseeable. Most courts have concluded that the duty to preserve arises once your company has "notice" that potential litigation is likely. But what constitutes "notice" triggering a duty to preserve electronic evidence depends on the circumstances. Clearly the service of a summons and complaint is "notice" imposing a duty to preserve. In some courts, a demand letter alone is enough to impose a duty to preserve. Courts have found other events to constitute "notice" and therefore impose a duty to preserve. A regulatory agency's adverse action with respect to a consumer product may constitute notice that consumer litigation is foreseeable. An employer's notice of employee's filing a charge with the EEOC has been held to

constitute "notice." An explosion at the company's manufacturing facilities involving property damage or personal injuries may be sufficient "notice" in some jurisdictions.



Norm Zivin: Spoliation simply is the failure to preserve evidence once a party is on notice that litigation is imminent. Spoliation is a long-standing doctrine and is applicable to both paper and electronic evidence.

Bill O'Neill/Matt Rechner: Spoliation includes "the destruction of records which may be relevant to ongoing or anticipated litigation, government investigation or audit." The Sedona Conference® Glossary: E-Discovery & Digital Information Management.

## How is electronic data subject to spoliation?

Stephen Rathke: Spoliation does not occur when you hit the delete button. ("Delete" is the biggest lie on the keyboard.) When you delete, you are really moving data to make more space. Spoliation may occur when a knowledgeable person actually eliminates data or when a data system automatically eliminates or overrides documents and email pursuant to a pre-existing document retention policy.

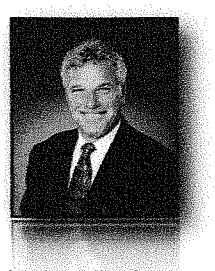
Joe Cohen: Electronically stored information has greater portability and wider distribution than paper stored information. An email you create at work sent to someone outside the company, for example, winds up being stored in multiple places in addition to your "sent" file and the recipient's "received" file. It can reside on your email server as well as the recipient's, your internet service provider's computer as well as your recipient's, and it can reside on back up systems at your company as well as the recipient's. Thus, more areas exist to search for potentially relevant information. And since most computer systems are designed for changing, writing over and obliteration of some or all of electronically stored information, a company's failure to preserve may, at the very least, invite a costly investigation into the circumstances under which the information was lost or destroyed and may lead to sanctions or to a spoliation instruction to the jury.

Bill O'Neill/Matt Rechner: Electronic data is particularly susceptible to spoliation due to the inherent and necessary characteristics of a computer's operating system. When saved data is no longer needed by the operating system (such as when a function has been completed) or when "visible," saved data is tagged by the computer's user for deletion, the operating system does not permanently erase the data. It simply ignores the data. The data is moved and rendered "invisible" to the operating system, but it remains resident on the computer's hard drive. When the operating system needs to save new data in order to perform a function, the operating system will randomly overwrite this "invisible" data that has been designated for deletion. Therefore, as a result of the necessary and normal workings of a computer's operating system, electronic data (both visible and "invisible") is constantly being created, saved and overwritten. If this electronic data is potentially relevant to an ongoing or anticipated litigation matter and proper steps are not taken to prevent the overwriting of this data, a party could be exposed to spoliation claims.

Geoff Bridgman: Electronic data is subject to spoliation in the same general ways as other physical evidence insofar as it may be altered, deleted or destroyed. As noted above, the very nature of the medium raises special problems because electronic documents are often continually overwritten and modified in a way that is simply not possible with traditional paper copies. On the other hand, it is often possible, at great expense, for forensic specialists to recover lost data.

**What special problems exist regarding emails?**

Stephen Rathke: Emails say the darndest things. People write things in emails that they never would say in a letter or in face-to-face conversation. Employees may send them to many recipients and groups within the organization. Recipients forward them to others. Worse, they sit in the computer infinitely longer than a scribbled note would last. Perhaps the most famous email in litigation history is the query of an executive of the drug company making Fen-phen: "can I look forward to my waning years signing checks for fat people who are a little afraid of a silly lung problem?" Guess the answer.



Jeff Shapiro: Special problems exist because individuals, for the most part, do not maintain e-mails and/or print hard copies. E-mails are more likely to be discarded than hard copies of documents because they are typically deleted once sent and read. E-mails should be treated like any other document knowing they may one day be disclosed. Also, individuals at every organizational level have a tendency to be far more informal in e-mails than in letters. As a result, e-mails may prove to be more damaging than an official letter or memorandum.

Joe Cohen: Emails and electronic information are also problematic because of something called "metadata." This is usually hidden to the naked eye, but it is present in many emails and especially in text files and spread sheet files attached to emails. Metadata may contain information about who was blind copied on an email, which computer generated the email or the file attached, prior revisions to attachments as well as edit dates (and by whom). Microsoft Word, for example, embeds all redlined changes into the text files it creates, although a program exists to "wash" it of this data.

Paul Gale: String emails are also problematic. They can pinpoint each participant to an extended discussion; when that person read the email; how long it took to respond; who received blind copies; who received the compete text from the prior sender (or edited text), etc. In general, emails are a trial lawyer's dream exhibit.

Norm Zivin: The proliferation of email has greatly increased the number of "documents" which are potentially discoverable. Emails also are distributed to wider groups of recipients due to user groups and easy forwarding.

Bill O'Neill/Matt Rechner: Email allows attorneys and their clients to communicate quickly, easily and cheaply. However, the widespread use of email has also contributed to an increased number of inadvertent disclosures of privileged and/or work product protected communications. For instance, if emails are sent (or forwarded) to email groups or to individuals who may stand outside of the attorney-client relationship, the risk for inadvertent disclosures (and potential waivers of the privilege) is greater. Attorneys need to exercise discretion when communicating via email with their clients (particularly corporate clients) and caution their clients to take proactive steps to preserve the confidentiality of those email communications.

Geoff Bridgman: Our experiences with e-mails are similar to those reflected by the group. These problems fall into three broad categories -- the content of e-mail, the distribution of e-mail and the difficulty in locating relevant e-mails. People often use e-mail without an adequate recognition that it forms a permanent record of the interaction. Thus, we see personal notes, jokes, opinions etc. in the e-mails that the author would never think of putting in a letter. This can be particularly damaging in litigation. More, the medium is particularly suited for quick responses that are often sent without thinking through all of the issues that may need to be addressed. Likely the increasing prevalence of Blackberrys and Trios will increase this problem as people are reluctant or unable to draft detailed responses on the small and cramped keyboards. This can lead to hard evidence that someone important learned of something important and the only response was a cryptic blurb popped out on a Blackberry from an airport lounge. The "Reply to All" button not only contributes to the size of e-mail chains, but it can result in a breach of confidentiality. On several occasions, I have received e-mails from the opposing party when their attorney copied them on an e-mail to me and then the client hit the "Reply to All" button. I was then privy to communication intended for the attorney, not me. Similarly, it is not uncommon in large

organizations that someone will have forwarded an attorney's e-mail to people outside of the management group, with the result that the attorney client privilege may be waived.

## What sanctions exist for spoliation by a party to litigation?

Stephen Rathke: If the document or item is the subject of a discovery request and the spoliation occurs after litigation begins, the sanctions provided in the rules will apply. Spoliation may occur, however, innocently and before the parties even think of litigation. For example, a property owner may obey government orders to clean up a fire scene; a vehicle owner may junk his wrecked car. Because the defendant is later deprived of the ability to inspect the scene or the vehicle, the plaintiff may lose the claim. I represented a plaintiff in a fire case and gained summary judgment on liability because the property owner cleaned the scene the day before a scheduled inspection by my expert. Another common sanction is an adverse inference instruction at trial. These sanctions may occur even if the destruction of the evidence is entirely innocent, not negligent and motivated by good or benign intentions. If you want some latin: Omnia praesumuntur contra spoliatorem. Recognizing the realities of document retention systems, the recent amendments to Rule 37 provide that a court may not impose sanctions when documents are lost because of the operation of routine data procedures made in good faith. If a litigation hold was in effect and ignored, the party probably would not meet the good faith requirement.

Jeff Shapiro: Striking of pleadings (answer or complaint), the imposition of monetary sanctions, and a jury instruction whereby the jury is instructed to draw a negative inference that the spoliated evidence was damning to the party that discarded it.

Joe Cohen: Courts are losing their reluctance to hand out large monetary sanctions as a discovery sanction. These may include an award of attorney fees and costs to the other side, imposing the cost of the opposing party's expert witness fees, and where possible, cost to restore electronic data.

Paul Gale: California has a standard jury instruction that provides: "If you find that a party willfully [suppressed, altered, damaged, concealed, or destroyed] evidence in order to prevent its being used in this trial, you may consider that fact in determining what inferences to draw from the evidence." In addition to an adverse evidentiary inference, the California Discovery Act provides a broad range of sanctions for "misuse of the discovery process." The sanctions are potent and include monetary sanctions, contempt sanctions, issue sanctions ordering that designated facts be taken as established, or precluding the offending party from supporting or opposing designated claims or defenses, evidentiary sanctions prohibiting the offending party from introducing designated matters into evidence, and terminating sanctions that include striking part or all of the action, or granting a default judgment against the offending party. In addition, the California Rules of Professional Conduct and the California Business and Professions Code expressly and implicitly prohibit attorneys from participating in the spoliation or suppression of evidence, and attorneys found to have done so are subject to professional discipline.

Norm Zivin: New York is the home of the notorious Zubulake decisions relating to a party's duty to preserve evidence, see Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003) ("I"); 2003 WL 21087136 (S.D.N.Y. 2003) ("II"); 216 F.R.D. 280 (S.D.N.Y. 2003) ("III"); 220 F.R.D. 212 (S.D.N.Y. 2003) ("IV"); 2004 WL 1620866 (S.D.N.Y. 2004) ("V"); and 2005 U.S. Dist. LEXIS 4085 (S.D.N.Y. Mar. 16, 2005) ("VI"). As a result, the probability of sanctions for spoliation are much greater than in the past and the adverse outcome of a trial where spoliation is an issue is much more predictable. In Zubulake, the jury awarded some $20 million in punitive damages.

Geoff Bridgman: Washington courts have allowed an adverse inference or a rebuttable presumption as a remedy in spoilation cases. The court will examine the importance or relevance of the evidence and the culpability of the party in determining whether to employ the rebuttable presumption. Depending on the severity of the violation and the importance of the evidence, Washington courts would also likely use Washington's counterpart to FRCP 37(b)(2) to enter a default judgment or strike pleadings. In two recent products liability cases where defendants wrongfully withheld evidence, Washington courts affirmed severe sanctions--in one case awarding over $750,000 in fees and in the other granting an order

of default in a class action. Although these cases address withholding evidence as opposed to destroying it, it is likely that Washington courts would consider sanctions up to and including entering a default judgment against a party who intentionally destroyed important evidence.

## What remedies exist when a non-party to the litigation engages in spoliation?

Jeff Shapiro: Under Florida law, a party may institute a lawsuit for spoliation of evidence against the spoliating "non-party" and recover the damages to which it would have been entitled if it had succeeded on its underlying claims. Further, a defendant may assert an affirmative defense of spoliation which, if proven, could act as a complete bar to a plaintiff's claims if the spoliation significantly hindered the defendant's inability to defend.

Joe Cohen: In most jurisdictions a "subpoena" is tantamount to a court's order to produce responsive information. Most courts treat the failure to comply with a subpoena as contempt of that court. Depending upon the circumstances, a court could hold a third party in contempt for destroying information after receipt of the subpoena. A finding of contempt could result in substantial fines, and where possible, orders to reconstruct the destroyed data. We're now seeing litigants issue "preservation" subpoenas to third parties in an effort to coerce those parties into taking extra steps to make sure they do not destroy any evidence responsive to the subpoena. Clients who find themselves as a third party on the receiving end of a subpoena or preservation order in someone else's lawsuit would be well advised to seek counsel's review of the scope and depth of such order. Federal Rule of Civil Procedure 45 allows the recipient of a subpoena to seek a protective order limiting the scope of discovery and, where appropriate, reimbursement for extraordinary costs that might otherwise be incurred in complying with the subpoena.

Paul Gale: California does not recognize the independent tort of spoliation of evidence. However, monetary sanctions are available against the non-party who engages in spoliation. Further, under the California Penal Code, it is a misdemeanor to knowingly conceal or destroy evidence that would otherwise be required to be produced in a legal proceeding.

Norm Zivin: Theoretically, a court could sanction a third-party for spoliation of evidence but this is unlikely unless the evidence was destroyed after service of a subpoena on the third-party.

Bill O'Neill/Matt Rechner: Sanctions can also be imposed against third-parties that fail to preserve and retain discoverable electronic evidence in response to a subpoena. In fact, the recent amendment to Rule 45(d) of the Federal Rules of Civil Procedure specifically address a third-party's obligations (as well as available safe harbors when electronic data is not reasonably accessible) when responding to a subpoena for the production, inspection, copying, testing and/or sampling of "electronically stored evidence." If a third-party fails to preserve "electronically stored evidence" after receipt of a proper subpoena, that party could be subjected to sanctions for spoliation.

Geoff Bridgman: The key element here is whether the person or entity has a duty to preserve evidence. Absent violation of a subpoena, the trial court in the underlying action would have no jurisdiction to impose a penalty on the third party that spoliated the evidence, although the aggrieved party might be able to file an independent tort claim against the person or entity who destroyed evidence. Generally speaking, a third party has no duty to preserve evidence, especially when the property belongs to the third party because imposing a duty interferes with that party's property rights.

A court might sanction one of the parties if the court concludes that the party had a right to control the third person or entity. Examples include when a parent company is party to a lawsuit and one of its subsidiaries has relevant documents and then destroys those documents, or when an accountant, lawyer or other professional receives a subpoena for client files and then destroys those files. In those cases, the court likely could not sanction the person or entity that destroyed the evidence, but would likely impute the act to the party to the litigation and employ whatever sanctions are available in the jurisdiction.

**Draft a Request for Documents which includes electronically stored data.**

Jeff Shapiro: Documents, materials, correspondence, notes, charts, and e-mails, including all metadata and prior versions/ forms of the documents, materials, correspondence, notes, charts. Another request would be for "all electronically stored and maintained documents, whether on-site or off-site, including all hard drives, Blackberries, cell phone data, and the like, that contain information regarding the issues in the case."

Joe Cohen: A prerequisite to a formal discovery request is gathering information from the adverse party concerning its computer systems, where data is stored, how it is stored (e.g., tape, hard drives, servers) and discussion about costs of retrieving the information desired. Where the opposition is uncooperative, interrogatories to obtain the information or an early oral deposition of the other side's IT manager may be necessary.

Paul Gale: Interrogatories are an inexpensive means of assessing the sufficiency of a party's production of electronic information. Like the Rule 30(b)(6) deposition, the interrogatories can focus on the opposing party's software, document retention policies, identification of IT personnel, system configuration and hard drive access.

Bill O'Neill/Matt Rechner: We like to pre-define the scope and grouping of an adverse party's "Relevant Computers," usually in a pre-litigation or early litigation preservation letter. An adverse party's "Relevant Computers" would include all hard drives from the desktop, laptop and/or notebook computers for particular individuals (to be specifically named in the preservation letter), personal digital assistants ("PDAs") for these same individuals, removable media devices (e.g., computer disks, CDs, DVDs, etc.), data and email servers, backup tapes and any other electronic media in the possession of the adverse party for a particular time period. Once the scope of the "Relevant Computers" is defined, a request is sent for mirror image copies of the adverse party's Relevant Computers. This request can be complimented by a contemporaneous request for access to the adverse party's Relevant Computers. If the adverse party refuses to produce the mirror image copies, you can press the adverse party (and the court through a motion to compel) to allow your own computer forensic expert to image the Relevant Computers.

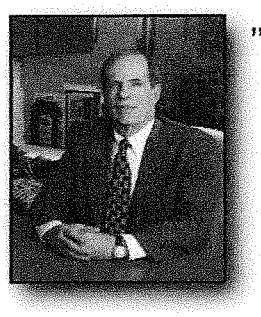
Geoff Bridgman: Set forth below are our standard definitions, which we will modify as necessary for the individual case:

> "Document" or "documents" means writings of every kind and character fixed in any tangible medium whatsoever, including, without limitation, the original and any copy, regardless of origin or location. Documents also includes documents in computerized form as defined in C below and any documents stored/reduced to storage on microfilm or microfiche.
>
> "Computerized form," "electronic data" and/or "computer files" means all data and information stored on, for use with, or for use on, mainframe computers, minicomputers, personal computers, desk top computers, laptop computers, notebook computers, portable computers, personal digital assistants, and computer networks or network workstations, including without limitation the following:
>
> (i) All data and information on, in, or retrievable from hard disk drives, hard disks, fixed drives, CD-ROM drives, tape drives, external drives, removable drives, portable drives, Zip/Jazz drives, including any internal back-up and archive systems; and
>
> (ii) All removable electronic media used for data storage including floppy disks or diskettes, cartridges, magneto-optical disks, CDs, Zip/Jazz disks, and mag-

netic tapes, including electronic storage media used for back-up and archiving data.

## At what point should the attorney expecting to defend a claim take action regarding client data?

Stephen Rathke: As soon as the attorney expects to defend the claim. It is very hard to deliberately destroy electronically stored documents. The real problem is the document retention policy which may destroy or reduce the availability of documents pursuant to the policy. The attorney has to do something to prevent the policy from destroying documents. The attorney also has a responsibility to monitor the "litigation hold" to insure compliance. Zubulake V, 2004 WL 1620866 (S.D.N.Y. 2004). If documents continue to drift into cyberspace in spite of a litigation hold, really bad things happen. See United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21 (D.D.C. 2004).



*"The attorney has to do something to prevent the policy from destroying documents."*

Jeff Shapiro: At the outset of the litigation or, at a minimum, immediately upon the receipt of discovery requests, the attorney must find out if the company has document maintenance/retention procedures in place and, if so, their substance. If the attorney has an ongoing relationship with the company, the attorney could help the company create its document maintenance/retention procedures.

Paul Gale: As soon as it appears that litigation may ensue, it is essential to meet with the client to make an initial assessment regarding electronic discovery. Counsel must determine how the client conducts its daily business. How are documents created? How extensively is e-mail used? It is imperative to determine the strengths and weaknesses of the client's electronic document preservation practices. Many companies either do not have well-developed document preservation policies or do not follow them closely. Knowing the client's practices in advance will help protect the client's interest when the scope of e-discovery is negotiated with opposing counsel.

Norm Zivin: In view of Zubulake, it is imperative for litigation counsel to instruct his or her client about presentation of evidence at the time a lawsuit is started.

Bill O'Neill/Matt Rechner: Unfortunately, there is no bright line rule regarding when attorneys need to coordinate with their clients to preserve and retain potentially relevant and discoverable electronic information. Consistent with the Judge Scheindlin's directives in Zubulake V, attorneys and their clients would be best served to undertake the "affirmative steps" detailed in that opinion to initiate a litigation hold and preserve potential electronic evidence as soon as litigation is "reasonably anticipated."

Geoff Bridgman: As soon as a claim is anticipated to preserve relevant documents and evidence. Not only does this avoid potential problems with the other side making a spoliation claim but it also helps ensure that your client will not lose the evidence that can help establish its case.

## Describe the roles of in-house and outside counsel regarding their client's data.

Stephen Rathke: In-house counsel must understand how an on-going document retention policy can cause spoliation. As soon as outside counsel gets involved, he or she must determine the status of all data. If outside counsel meets resistance within the company, the stage is set for disaster. Therefore, outside counsel must have the cooperation in those within the company if the claim is to be successfully defended.

Jeff Shapiro: In-house and outside counsel must coordinate efforts to ensure that appropriate procedures are in place for document maintenance/retention whereby the employees understand their responsibilities with respect to electronic data retention and/or retrieval.

Paul Gale: In-house and outside counsel must identify personnel within the company who may possess relevant information, and notify those individuals to preserve all relevant documents. It also may be necessary for the client to both suspend any computer programs that automatically delete electronic documents or e-mail relevant to the litigation and preserve all backup tapes containing relevant information until the litigation is resolved.

Norm Zivin: Most in-house counsel are aware of the duty to preserve evidence. They must be on the front line of dealing with the clients personnel. However, outside counsel has an affirmative duty under Zubulake to ensure that this task is undertaken and that there has been compliance by the client.

Bill O'Neill/Matt Rechner: In-house counsel can serve as an invaluable liaison between outside counsel and the client's Information Technology ("IT") personnel. Both in-house and outside counsel know (or should know) the legal requirements and ramifications surrounding the preservation of electronic data relevant to a lawsuit. IT personnel, on the other hand, are generally more focused on the day-to-day operations of the client's computer network, including such tasks as hard drive repairs or replacements, the periodic recycling of client backup tapes, routine server maintenance, etc. Outside counsel can sometimes encounter resistance from a client's IT personnel when they are directed by outside counsel to suspend these types of everyday tasks as a result of a "litigation hold." As an intermediary, in-house counsel can work to ensure that outside counsel and the client's IT personnel are working together cooperatively and effectively.

*"In-house counsel can serve as an invaluable liaison between outside counsel and the client's Information Technology ("IT") personnel. "*

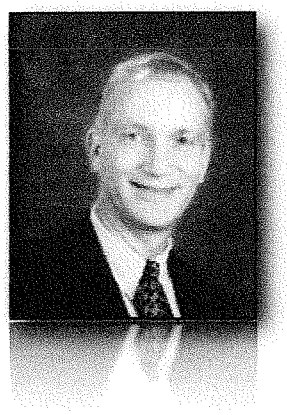
Geoff Bridgman: Long before litigation is anticipated, in-house counsel has an important role to play in helping to establish document retention policies and policies regarding how confidential or sensitive documents are shared to preserve confidentiality. Once litigation is anticipated, in-house counsel should advise key personnel and IT staff to take affirmative steps to preserve relevant evidence, including electronic evidence. Outside counsel needs to work with in-house counsel at the outset to obtain documents needed for the defense and to help ensure that documents are not lost or destroyed. As litigation progresses, outside counsel needs to keep in-house counsel advised as new issues arise to ensure that documents that might not have seemed relevant at the outset, but that are now relevant are protected.

---

**What are some sources of information and guidelines regarding the management of electronic data?**

Stephen Rathke: Companies have sprung up which offer litigation services. E.g., see www.krollontrack.com . These companies have an alarmist tendency which coincides with a marketing strategy, but they may be helpful both for locating your own data and also for guidance in creating a discovery strategy. Another issue which cries out for a consultant involves the use of cell phones and Blackberry—like devices. Very few lawyers are sufficiently up-to-date to deal with cutting-edge technology.

Jeff Shapiro: Westlaw and Lexis-Nexis maintain articles and reports regarding the management of electronic data. Further, there are IT companies that devise systems and put procedures in place in accordance with the client company's needs.



*"In the lawsuit context, most top-flight trial law firms have developed a significant amount of expertise in addressing electronic discovery issues."*

Joe Cohen: In the lawsuit context, most top-flight trial law firms have developed a significant amount of expertise in addressing electronic discovery issues. Many now either employ or partner with electronic information storage and retrieval talent to bring a comprehensive solution to the client's litigation needs. Firms experienced in this are likely to be more cost effective for the client in the long run, because they not only know and understand the legal and fact issues in the case, but also are able to counsel the client in responding to electronic discovery issues as well as finding the nuggets of gold in the other side's electronic files.

Paul Gale: Consistency is extremely important in electronic discovery. The process will run much more smoothly if one is able to follow a structured procedure for retrieving, storing, reviewing, cataloging and producing documents. There is a fast-emerging market of computer software technology to aid trial attorneys in managing and utilizing electronic information in discovery. Databases such as Summation® and Concordance® are among the most popular. Other software firms creates ad hoc data bases and have indexing and key-word searching capabilities.

Norm Zivin: Although there are services which are happy to manage electronic data for litigation, one must bear in mind that these services are very expensive and usually are unnecessary except in a very large case.

## What are some strategies for mitigating the time and expense involved on producing electronic data?

Stephen Rathke: If both sides have an understanding of what they have and where it is stored, they may be able to reach agreement concerning the parameters of electronic discovery. The recent amendments to the federal rules incorporate these concerns into the Rule 16 meeting. If agreement cannot be reached, one can approach the court at an early discovery conference to try to keep things in line and shift the costs to the requesting party.

Joe Cohen: Address the issue early with the opposition, and marshal the information necessary to ask the court for protection if the opposition acts unreasonably. Frequently, counsel can negotiate a discovery plan that minimizes a company's costs.

Paul Gale: Negotiating a comprehensive stipulation between the parties is critical to achieving a successful electronic discovery process. Given the huge volume of electronic documents created over the span of the litigation's relevant time period, it is in everyone's best interest to agree to the scope of electronic discovery. Without such an agreement, discovery costs could spin out of control. If opposing counsel refuses to cooperate, I would move for a protective order before producing any discovery and in the motion propose a reasonable electronic discovery plan that would govern for the duration of the litigation.

Norm Zivin: Most courts are not as interested in supervising production of electronic information as the judge in Zubulake. For the most part, it is up to the respective counsel to be reasonable in negotiating what is truly necessary.

Bill O'Neill/Matt Rechner: More and more courts are helping to mitigate the time and expense of electronic discovery by appointing a neutral, third-party computer forensic expert to work with both the plaintiffs and defendants in a particular case. See e.g., Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999); Simon Property Group v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000), Experian Info. Solutions, Inc. v. I-Centrix, L.L.C., Case No. 04 C 4437 (N.D. Ill. July 21, 2005). This neutral-expert approach will likely become more prevalent with the recent amendments to the Federal Civil Rules which make electronic discovery a required component of every court's case management plan.

Geoff Bridgman: Make an early assessment whether electronic data is likely to form a critical part of the case. If it is, you should consult with the client's IT department to ascertain the difficulty in retrieving data and consult with outside experts who can retrieve and compile the data. This gives you the information needed to try and work out a compromise on cost sharing with the other side, and if the other side is unreasonable, it gives you the basic evidence to support a motion for protective order.

*"Make an early assessment whether electronic data is likely to form a critical part of the case."*

## Describe some technical issues such as embedded data and duplicate data and how to resolve them?

Stephen Rathke: Embedded data may be relevant if the drafting history of a particular document is at issue. An attorney needs technical assistance from a computer forensic specialist. If the search is for an internet document, the web page may have many changes since the relevant time period.

Jeff Shapiro: These issues can be resolved by having an IT department that is aware of what data is required to be retained and maintained. Thus, embedded data will be accessible, if necessary.

Joe Cohen: A number of companies have software that purports to "strip" files of metadata before a file is sent out of the company (e.g., by email). A company would be well advised to preserve and not to destroy metadata.

Paul Gale: In certain cases, it is necessary to retain forensic experts. The court may appoint a forensic expert where the amount of electronic data to be produced is significant. Forensic experts have also played critical roles in cases where parties have fabricated electronic evidence. A case in point is Premier Homes & Land Corp. v. Cheswell, Inc., 240 F. Supp. 2d 97 (D. Mass. 2002). There, plaintiff's claim was largely based on a single e-mail. Defendants contested the authenticity of the e-mail and filed an ex parte motion to "preserve certain evidence and expedite the production of electronic records." The court ordered defendants' experts to mirror-image plaintiff's computer hard drives, backup tapes and other data storage devices. Soon thereafter, plaintiff admitted to his attorney that the e-mail had been fabricated by pasting most of a heading from an earlier, legitimate message and altering the subject matter line. The court granted defendants' motion to dismiss, finding that the plaintiff willfully engaged in a scheme to deceive the court. Monetary sanctions also were assessed against the plaintiff.

Norm Zivin: When documents are prepared using Microsoft Word, a history of changes is created. One must be cognizant of that feature in producing and transmitting electronic versions of documents.

Bill O'Neill/Matt Rechner: "Metadata" is one of those buzzwords getting more and more attention these days. Metadata is essentially "the data behind the data." It is the information that describes how, when and by whom a particular set of data or document was created, accessed, deleted, revised, modified and/or formatted. Some metadata is viewable by a computer user. Other metadata is hidden or embedded. However, whether visible or invisible, courts are requiring parties to preserve (and, in some cases, produce) this metadata in the course of electronic discovery. See e.g., Williams v. Sprint/United Mgmt Co., 230 F.R.D. 640 (D. Kan. 2005) ("when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."). Attorneys must be cognizant of the existence and content of any underlying metadata when producing electronic data to an adverse party.

Geoff Bridgman: Sadly, there are no easy answers on how to handle such hidden data. While Joe advises it is wise to keep the metadata, an argument can be made that it is equally wise to have systems in place to strip the data especially in e-mails. So long as the system was in place before litigation is anticipated, it really becomes part of a company's document retention policy. In some respects it is no different than having a policy of destroying drafts and retaining only complete documents. More, it is possible that a client will inadvertently disclose confidential information contained within the metadata but not otherwise observable. This raises a related issue, namely that in producing electronic discovery, care must be taken to review the metadata as well to ensure that attorney-client or other confidential information is not hidden within the document.

## How can privileged information and communication be protected?

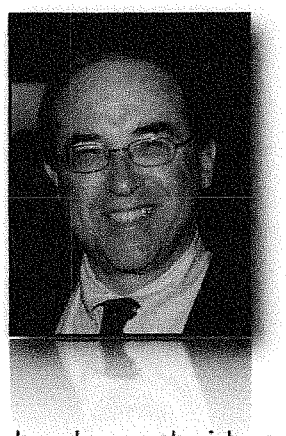
Stephen Rathke: The old fashioned, tedious way: reviewing the document before it is produced. Search technology may help. Getting a handle on the documents and collecting them may be such a chore that the documents (and their many copies) may not be adequately reviewed before they are produced which results in the inadvertent disclosure of privileged material.

Jeff Shapiro: Privileged information and communication does not lose its privilege by virtue of it being electronic. However, policies should be in place to see to it that the privilege is not destroyed by sharing the document with someone whose status could eliminate the privilege. For example, electronic documents should not be shared with non-employees (IT technicians) if that would destroy the privilege.

Joe Cohen: Emails and paper information are somewhat easier to identify as possibly containing attorney client privileged information. It requires identification of the person(s) who may have served as counsel and isolation emails to and from such persons. In the end, most courts will eventually require a privilege log, and someone will have to review for confidential information.

Paul Gale: A protocol must be developed for electronically screening out privileged documents from production. This can be accomplished through the use of search terms such as attorney and firm names, and the phrases "work product" and "privilege." At the end of the day, however, counsel must make sure that these documents are, in fact, privileged by reviewing them separately.

Norm Zivin: There is no substitute for old-fashioned page-by-page review. Lawyers are not always identified by name (perhaps only by email address), and lawyers' advice may be transmitted between company executives. No computer program will cull this information.



*"Lawyers are not always identified by name (perhaps only by email address), and lawyers' advice may be transmitted between company executives. No computer program will cull this information."*

Bill O'Neill/Matt Rechner: Given the vast amount of data that may be exchanged in the course of electronic discovery during a lawsuit, there is an increased risk of inadvertent disclosures of privileged and/or work product protected communications and documents. In the past, parties have traditionally entered into non-waiver agreements whereby each side agrees that if privileged documents are mistakenly disclosed, the receiving party shall return the privileged materials to the producing party and the inadvertent disclosure shall not constitute a waiver of the attorney-client privilege. A recent federal court decision Hopson v. Mayor and City Council of Baltimore, 2005 WL 3157949 (D .Md. 2005), expounded upon this practice with increased skepticism though. In Hopson, the court asserted that these types of non-waiver agreements do not obviate a party's duty to conduct a pre-production privilege review of its electronic documents. To fully protect themselves, the Hopson court recommended that parties should request and obtain a court Order: (1) detailing the privilege review procedures to be followed by the parties concerning electronically stored information and (2) specifically providing that, if a party complies with those procedures and nevertheless inadvertently produces privileged information, this inadvertent disclosure will not result in the waiver of any privilege or work product protections. In essence, no waiver results because the inadvertent disclosure occurred pursuant to a court order.

Geoff Bridgman: Absent agreement from the other side, each document must be reviewed for privilege. Clearly, the more efficient approach is to reach agreement with the other side and have the agreement adopted as a court order. Two approaches are commonly used, the so called "clawback" and the "sneak peek." The clawback allows a party to produce documents and if it later discovers that it had inadvertently produced a confidential document, the other side must return the document. The sneak peek allows the requesting party to review documents or data from a large collection and mark what it wants produced. The producing party then reviews for privilege those documents that were selected for production. We typically use a "clawback" agreement.

---

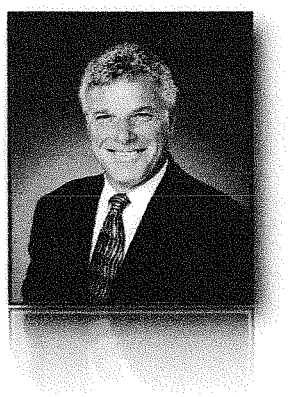
## Are the Zubulakes the first and last word? Critique Judge Scheindlin's decisions. How has your jurisdiction dealt with the issues addressed in the Zubulakes?

Stephen Rathke: Minnesota cases have not dealt with the Zubulakes. In those five cases, the judge provides many guidelines, not only for those litigants, but also for litigants everywhere. While guidelines are appreciated, I wonder whether this one-person rule-making committee decided too much without the benefit of the input that should be expected of rule-making bodies. The amendments to Rule 26 of the federal rules address the cost-shifting principles in a manner roughly consistent with Zubulake. Revised Rule 37 precludes sanctions where the loss of data is due to a routine document procedure applied in good faith. Once a duty to preserve arises, however, further routine destruction of data would not be considered good faith. Another source of information is the work of the Sedona Conference at www.thesedonaconference.org.

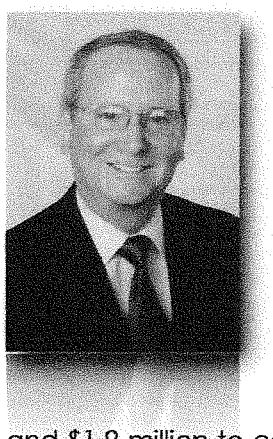
Jeff Shapiro: The Zubulakes, although groundbreaking, are not necessarily the last word in the production of electronic documents and data. Judge Scheindlin's decisions may not be applicable to every

case involving electronic data and documents. The Zubulake decisions contain a punitive element directed against UBS Warburg due to its discovery violations (note that Zubulake herself had documents that she kept that UBS Warburg did not produce, and UBS Warburg operates in a heavily regulated industry relative to document retention). Despite the factual peculiarities of the Zubulakes, they provide a solid baseline for a discovery approach particularly when faced with an overwhelmingly large document production. Currently, no Florida state court cases reference or interpret the Zubulakes.

*"The Zubulakes, although groundbreaking, are not necessarily the last word in the production of electronic documents and data."*



Joe Cohen: The decisions in Zubulake are subject to the recent amendments to the federal rules which go into effect December 1, 2006. Rule 16 requires early discussion with the court regarding electronic discovery issues. Rule 26 provides that a party's initial disclosures include "electronically stored information" relevant to the party's claims or defenses. Rule 26(f) will require the parties to address preservation up front. Rule 37 addresses sanctions and states that, absent exceptional circumstances, sanctions may not be imposed if electronically stored information sought in discovery has been lost as a result of the routine operation of an electronic information system, so long as that operation is in good faith.



*"A protocol must be developed for electronically screening out privileged documents from production. "*

Paul Gale: California Code of Civil Procedure Section 2031.280 provides: "(a) Any documents produced in response to an inspection demand shall either be produced as they are kept in the usual course of business, or be organized and labeled to correspond with the categories in the demand. (b) If necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form." In Toshiba America Electronic Corporation v. Superior Court, 124 Cal. App. 4th 762 (2004), a misappropriation of trade secrets case, plaintiff filed a motion to compel defendant to produce responsive documents from 800 backup tapes, which would have cost between $1.5 and $1.9 million to compile. Citing Section 2031.080, the defendants argued for cost-shifting due to undue burden. The plaintiff contended that under Zubulakes, cost-shifting in these circumstances was inappropriate because the plaintiff should not be penalized for defendant's decision to keep its records in a manner that made them difficult to retrieve. The trial court granted the plaintiff's motion without explanation. On a petition for writ of mandate, however, the Court of Appeal issued the writ, holding that the demanding party was responsible for the reasonable expenses incurred by the responding party in translating the data compilations into a reasonably usable form. The Court of Appeal was not unsympathetic to the plaintiff's position, but held that it was bound to follow the Legislature's mandate as codified in Section 2031.

Bill O'Neill/Matt Rechner: The Zubulake decisions, while the most prominent cases in the area of electronic discovery, are certainly not the final word on this issue. Like most areas of law, courts have the discretion to apply (and have already applied) e-discovery principles differently on a case-by-case basis. For instance, some courts may be less inclined to hand down the types of discovery sanctions ordered by Judge Scheindlin against UBS Warburg in Zubulake IV and V. Similarly, some judges may elect to impose less stringent requirements upon attorneys as compared to Judge Scheindlin's directives in

Zubulake V. This discretion is underscored by the open-ended language of the December 1, 2006 amendments to the Federal Rules of Civil Procedure. In Ohio, one important e-discovery case is Hayman, et al. v. PricewaterhouseCoopers, LLP (In re Telxon Securities Litigation), 2004 U.S. Dist. LEXIS 27295 (N.D. Ohio July 2, 2004). In connection with the Telxon Securities class-action litigation, the Securities and Exchange Commission ("SEC") requested documents from PricewaterhouseCoopers ("PWC") relating to its financial audit of Telxon. The class plaintiffs and Telxon subsequently moved the court for sanctions against PWC, alleging that PWC failed to preserve and produce all relevant electronic documents and databases, including emails and metadata, in response to the SEC's request. The federal magistrate concluded that since PWC had been on notice of the SEC's investigation and was obligated to preserve this electronic evidence, its failure to do so was intentional spoliation. As a result of PWC's bad faith conduct, the magistrate recommended to the district court that default judgment be entered against PWC on the issue of liability. Not surprisingly, the parties settled this litigation shortly after the magistrate's report and recommendation was issued. The total settlement amount was just shy of $68 Million.

Geoff Bridgman: Washington Courts have not adopted any of the Zubulake decisions, and as noted above they are only persuasive, not mandatory authority. They are more likely to be the "first word" rather than the "last word" in electronic discovery. Judge Scheindlin's careful analysis of the factors relevant in cost sharing provides a useful framework. The imposition, however, of duties on counsel: to learn the intricacies of a client's computer network and back-up systems; to interview all witnesses disclosed in the mandatory lay down disclosure; to issue a "litigation hold"; and to monitor the client for compliance ignores the reality of most litigation. Read literally, the court is imposing a requirement that defendants must spend many tens of thousands of dollars in attorney fees educating outside counsel about the intricacies of the client's computer network and interviewing all key witnesses. Imposing such an expense at the outset of each case before the client can ascertain the risks of the case is unfair and, for most cases would be grossly inefficient.

## How does all this impact clients in jurisdictions outside the United States?

Jeff Shapiro: Clients outside of but subject to suit within the United States will likely be confronted with the same spoliation standards as American companies if sued in the United States. Thus, they should also be made aware of the potential risks of spoliation and take necessary precautions.

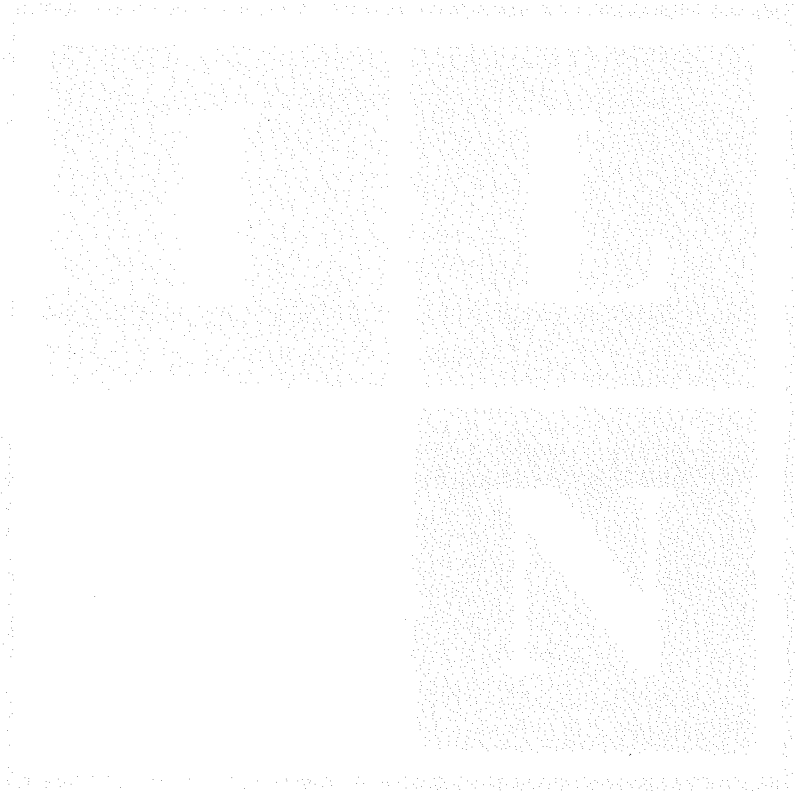
Joe Cohen: The impact on multi-national companies is tremendous. Many do not have central storage of electronic information, and instead rely upon multiple systems around the world. Often there are language, programming, and other technology issues that differ from one part of the world to another. A number of countries have privacy restrictions on things we in America would not consider to be subject to privacy.

Norm Zivin: Many cases in federal courts involve foreign parties who are not cognizant of any need to maintain documents, especially those in electronic form. It is a challenge for outside counsel to convince a party from a country where discovery is limited or non-existent that every scrap of paper and every email must be preserved.

Bill O'Neill/Matt Rechner: Foreign privacy laws (e.g., the Data Protection Act of 1998 in Europe) create unique obstacles for multi-national clients who find themselves on the receiving end of an electronic discovery request. In these types of special circumstances, attorneys should look beyond local e-discovery experts and retain a company with greater experience in international e-discovery matters, such as Kroll Ontrack (www.krollontrack.com) or LECG, LLC (www.lecg.com).

Geoff Bridgman: If the company is subject to the jurisdiction of U.S. Courts, the impact is the same as for any other domestic litigant, although educating the client as to the need to protect documents may be more difficult if it is unfamiliar with American discovery practices. Different languages and different networks make electronic discovery extremely expensive and time consuming. Multi-national companies can try and mitigate the burden of preserving and producing electronic evidence by establishing

U.S.-based subsidiaries and carefully ensuring that all contracts and other actions that have the potential for litigation are run through the U.S. subsidiary. Legitimate arguments can then be made that the subsidiary does not control or have a right of control over its parent or its computers. This strategy has potential downsides, however, that a court might disregard the separate entities and hold the subsidiary liable for any documents the parent lost.



**For more information about the International Lawyers Network please contact:**

**Mr. Alan Griffiths**

**Executive Director**

**Tel: 201.594.9985**

**Email:** alangriffiths@iln.com

**Ms. Lindsay Griffiths**

**Director of Network Development**

**Tel: 201.594.9430**

**Email:** lindsaygriffiths@iln.com